VERMONT

Agency of Human Services Privacy Considerations

Your department, unit, division or program must take reasonable steps to protect privacy and in so doing comply with the AHS HIPAA Standards and Guidelines at http://intra.ahs.state.vt.us/centralsupport/hipaa/hipaa_standardsandguidelines and state policies.

Consider:

- Personal information--information which individually identifies a person--should flow and be stored throughout the workspace in a deliberate manner. Think through what personal information, both in paper and electronic format, exists in the workspace, how it flows (for example, from the administrative assistant to the staffer to the filing room), and how it is stored. Think about paper files, word documents, excel spreadsheets and other documents containing personal information. Consider whether only those who need to see the personal information have access to it and whether it should be stored more securely.

- Some supervisors have found that simply asking staff on a one-to-one basis to think about the flow and storage of personal information in their work has encouraged staff to safeguard this information even more. Ask staff to think about what personal information they have in their office and on their PC, how they store it, and if it could be better stored. Supervisors find that after these conversations, staff consistently pick up print-outs and faxes; flip documents and files face down in mailboxes and on their desks; store files out of open view; and are generally more careful.

- Establish a process to monitor staff access to personal information. When staff shift jobs or their duties evolve, make sure their access to personal information, specifically health information, changes accordingly. Remember to have these staff revisit the AHS Health Information Survey at https://www.ahsinfo.ahs.state.vt.us/hipaa/survey/healthsurvey.cfm and work with their supervisors to revise their responses to accurately represent these changes.

- Only that information which is needed should be recorded in paper and electronic documents. For example, if all that is truly needed is an individual's name on the file folder, then staff should only include their name, and not their SSN or other identifying information.

- Paper files containing personal information when not in use should be stored securely. Files not in use should not be stored on desktops and instead should be stored in drawers or cabinets, which are locked. If locked drawers or cabinets can not be made available, consider locking the individual office when staff is absent or storing all files in a common file room that can be locked and/or is not accessible to the public.

- Files that are no longer needed that are stored in filing boxes or cabinets should not be located in hallways or common areas easily accessible to the public. Find a more secure location for processing before sending them to State storage.

- Incoming mail, print-outs, and faxes should be placed face-down in staff boxes. Outgoing mail and pink mail should be placed face-down in pick-up bins.

Mailboxes and pick-up bins should be placed in monitored areas that are not easily accessible to the public.

- Print-outs, faxes and copies should be routinely picked up. Assign an individual to make sure they are distributed on a routine basis.

- Paper documents containing personal information should be shredded on-site or placed in locked bins that are picked up to be shredded. They should not be placed in recycling bins. Consider buying a shredder or contracting if the shredding volume is large. Locate shredder boxes adjacent to printers and copiers so that documents are immediately shred. When shredders are not close to printers and copiers and are even just a short walk away, these documents often land in the recycling bin.

- Personal information in electronic format should be stored on servers. Staff should avoid storing personal information on laptop computers, desktop computers, diskettes, cds or unencrypted usb flash drives.

- Just as paper documents should be shredded, diskettes and cds that contain personal information should be physically destroyed. Staff should not simply throw them away. Equipment that is no longer needed that may contain personal information should be given to IT staff to “surplus.” This includes phones, usb drives, pdas, computers, laptops, and other electronic storage devices such as external hard drives. IT staff will make sure the items are securely erased before surplussing them.

- Staff should not log in using their own password and account so that others can use the computer, even if the "others" are temp staff or coworkers. Only the individual staff whose password it is should be using the account.

- Staff should lock their PC or laptop whenever they leave it unattended by pressing “ctrl-alt-delete” and then “k.”

- Passwords should not be written on post-its and stuck on bulletin boards, under keyboards or in other accessible areas. One division did a sweep of work areas to ensure that passwords were not stored in inappropriate places. They found a number of post-its with passwords written on them stuck under keyboards and on the backs of computers.

- Some supervisors have assigned one or two staff persons whose offices are near to the entrance of the workspace to act as “receptionists.” These receptionists monitor, greet and escort non-staff who enter the workspace. Consider arranging the workspace so that staff can act as “receptionists.” Train all staff to ask non-staff their destination and to escort them when necessary. This is especially important if there is personal information in the workspace.

- Windows to ground floor offices and other spaces such as porches, storage rooms and common areas must be closed and locked when staff leave for the night. If filing cabinets, file room, or office doors are to be locked at night by staff, assign specific staff to do so. Monitor that these are actually being locked.

- Establish a system for key distribution to new staff and collection from staff who are leaving employment. Store extra keys in a secure location.